

Serial No. 09/942,552

Debbie Ann Godwin

Page 4 of 7

Section III:
AMENDMENT UNDER 37 CFR §1.121 to the
DRAWINGS

No amendments or changes to the Drawings are proposed.

Serial No. 09/942,552

Debbie Ann Godwin

Page 5 of 7

Section IV:
AMENDMENT UNDER 37 CFR §1.121
REMARKS

Rejections under 35 U.S.C. §103

In the Office Action, claims 1 - 15 were rejected under 35 U.S.C. §103(a) as being unpatentable over US patent application publication 2002/0031134 to Poletto (hereinafter "Poletto") in view of "Intrusion Detection" by Escamilla (hereinafter "Escamilla").

Applicant requests withdrawal of the rejections and allowance of the claims as originally filed on the basis that the claims specify steps, elements, or limitations not taught by Poletto in view of Escamilla, and thus a rejection is improper under MPEP §2143.03, which states:

All Claim Limitations Must Be Taught or Suggested.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art.

In our claims, we have specified our "jumping window" which is employed to reduce over-reporting of violations. We have explained that with a simple sliding window approach (e.g. the window is moved forward by one event for each analysis step), multiple reports of violations are generated from a single set of failed login attempts in a short period of time (e.g. period shorter than the analysis window length). In such a situation, several window positions include a number of violation counts exceeding a threshold, which results in multiple alert messages, all of which are redundant except for one. (See our disclosure at pg. 6 lines 13 - 17)

Our system solves this problem by "jumping" our analysis window when the violation threshold is met for a particular window position. In this scenario, instead of simply moving the window ahead a single sample for the next round of analysis, our system advances the window to a point where it starts at the next event following the last event in the previous window. As such, the window is "jumped" forward to a position so that it does not overlap with the previous window position. (See our disclosure at pg. 6 line 14, pg. 10 line 20 - pg. 11 line 7, paragraph

Serial No. 09/942,552

Debbie Ann Godwin

Page 6 of 7

[0034], paragraph [0052], and fig. 6 #67).

In independent claims 1 and 6, we have specifically claimed (emphasis added):

...

responsive to said count exceeding a threshold, producing a violation message and jumping said float period by setting said start time to be equal to a time stamp value of an event in said event list immediately following said float period end time, otherwise advancing said float period by a single event by setting said start time to a time stamp value of an event in said event list immediately following said start time; and

...

In independent claim 11, we have specifically claimed (emphasis added):

...

a float period manager for advancing a float period from an initial position to a plurality of subsequent positions, said initial position having a float period start time equivalent to said earliest event time stamp and a float period end time equal to said start time plus a float period length, said float period being adapted to jump the float period to a subsequent position such that said start time is equivalent to a time stamp of an immediately subsequent event following said end time, and also being adapted to advance said float period to a subsequent position by a single event such that said start time is equivalent to a time stamp of an immediately subsequent event following said start time;

...

an evaluator for comparing said event count to a violation threshold, and responsive to said count exceeding said threshold, producing a violation message and causing said float period manager to jump said float period to a subsequent position...

Serial No. 09/942,552

Debbie Ann Godwin

Page 7 of 7

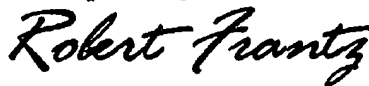
Poletta in view of Escamilla fails to teach suppression of over reporting by jumping an analysis window in this manner. In the Office Action, this aspect of our claims was not quoted, and no specific teaching of Poletta or Escamilla was cited for this aspect of our claims. A portion of Escamilla was cited for teaching a "moving average" process, but our claims specify a process that counts events up to a threshold, but which is not dependent upon or using an averaging process at all. Note especially that the example moving average document supplied by Examiner in support of the term "moving average" indicates a window which is advanced one sample or event for each iteration of analysis, including an averaging function (not threshold counting), but is silent as to jumping the analysis window as we have disclosed and claimed (line numbers and emphasis added to following quotation):

```
...
17   DO i = 1, Size-Window+1
18       Sum = 0.0
19       DO j = i, i+Window-1
20           Sum = Sum + x(j)
21       END DO
22       Avg(i) = Sum / Window
23   END DO
...
```

Note especially that the outer DO loop (lines 17 and 23) represents the advancing logic for the window position, which simply advances by one sample per iteration of the loop, and there is no logic for "jumping" the window by setting the beginning of the next window to the sample immediately following the last sample in the current window. Also please note that this is an *averaging* process (line 22), not a *threshold detecting* process.

For the foregoing reasons, applicant requests withdrawal of the rejections, and allowance of the claims as originally filed.

Respectfully,



Agent for Applicant(s)
Robert H. Frantz, Reg. No. 42,553
Tel: (405) 812-5613